FORS
explore.understand.share.

FORS Data Service Data Protection Policy

This document sets out the data protection policy of the FORS Data Service. It aims to clarify its missions, responsibilities, and activities with regard to the processing of personal data.

1. Definitions

Data controller: Natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Sub-contractor: natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller.

Personal data: all information relating to an identified or identifiable person.

Sensitive data: personal data on:

1. religious, ideological, political or trade union-related views or activities,
2. health, the intimate sphere, or the racial origin,
3. social security measures,
4. administrative or criminal proceedings and sanctions.

2. The FORS Data Service mission and responsibilities

The FORS Data Service mission is to acquire, preserve, and disseminate digital research data for the social science community in Switzerland. It is at the service of the researchers and institutions who wish to share and/or reuse empirical materials according to the principles of Open Science. It uses the SWISSUbase infrastructure as its main technical tool for the preservation and dissemination of data (except for replication data).

In order to carry out its mission, the FORS Data Service may have to process personal data. Two cases arise:

a. In order to ensure the administrative management of its activities, the FORS Data Service may need to process the personal data of its clients. In this case, the FORS Data Service acts as a data controller and is responsible for ensuring compliance with data protection laws. Please note that the responsibilities for the processing of personal data of SWISSUbase users are set out in its General Terms and Conditions of Use. These must be read and agreed to by the users at the time of registration on the platform.

b. It may happen that the datasets archived and disseminated by the FORS Data Service contain personal data. In this case, the FORS Data Service acts as a subcontractor in the sense that it processes these data on behalf of a third party (the person or the institutions that use the services of the FORS Data Service for the archiving and dissemination of their research data). As a subcontractor, the rights and duties of the

FORS Data Service are limited to those set out in the service contract (data deposit agreement), as well as the legal obligation to ensure data security. The legal responsibility remains with the data controller, usually the principal investigators (PIs) on behalf of their affiliated institutions.

Practices with respect to data protection

To help data depositors comply with data protection laws and clarify responsibilities, the FORS Data Service implements the following practices

- Data depositors are informed of their duties and are required to attest to the legality of the collection, deposit, and dissemination of the data.
- Basic checks are carried out in partnership with the research team (e.g., quality of informed consent, anonymisation, etc.). The FORS Data Service may ask to review certain documents (e.g., information sheets) and reserves the right to refuse datasets in case of ultimate non-compliance with data protection laws.
- Data depositors must sign a deposit agreement that distributes responsibilities.
- During the deposit process, data depositors choose the appropriate conditions of access to the data (more or less restricted).
- A data use agreement is drawn up which stipulates the conditions of use of the data, as well as the obligations of the data users.
- Transcripts of interviews in a text format are favoured over raw data in audio or video formats. However, the latter can be deposited on a case-to-case basis, provided that consent has been obtained to share such materials, and the fact that it is of value for re-use purposes.

Services with respect to data protection

a. During the project

The FORS Data Service provides data management support during the research project by means of individual consultancies, trainings, and the provision of written guidance such as the FORS Guides. Support includes key topics with respect to data protection, such as general guidance regarding ethics and data protection, as well as specific practices such as obtaining informed consent, data anonymisation, or securing access to data. Depending on demand and available resources, the FORS Data Service may also take up mandates to process and prepare data in line with the applicable data protection rules.

b. At the end of the project

Once data have been submitted for dissemination, the FORS Data Service provides basic checks, in particular whether the data and related metadata and documentation are complete, and whether data protection obligations appear to be met (e.g. quality of anonymisation, informed consent, etc.). The checks carried out by the FORS Data Service are

advisory and in no way relieve data depositors of their responsibilities as data controllers. At the time of deposit, it is up to the PIs or institutions to guarantee the legality of the collection, storage, and dissemination of the data they submit.

Based on the choices of the depositors, the FORS Data Service makes available data use agreements that define the conditions of use and ensure data protection. The data depositors are offered the possibility to choose between restricted contracts and CC licences, and FORS recommends limiting restrictions and choosing licenses that are as open as possible. It is the depositors' responsibility to ensure the lawfulness of their choice (ideally by submitting it to the legal departments of their institutions). The FORS Data Service cannot be held responsible for non-compliant choices regarding access conditions.

Finally, if needed to strengthen the protection of individuals whose data is disseminated, the FORS Data Service offers the possibility to set up restrictive access conditions (e.g. use for certain purposes only, prior agreement by the PIs, etc.). Furthermore, the FORS Data Service also offers the possibility to fix an embargo period.

c. At the time of data dissemination

The FORS Data Service ensures that the data are stored on facilities that apply high security standards when it comes to granting access, backing-up, and preserving the data. Currently, data are stored on the servers of SWITCH. Should data be stored using a different infrastructure in the future, the FORS Data Service will make sure that at least the same level of security will be met.

Based on the deposit agreement, some datasets can only be distributed after prior approval of the person/institution who is responsible for the data (i.e., the PI, data producer, or assigned third party). Should the person responsible for the data no longer be able to grant access to the data (for example in case of retirement or death), the FORS Data Service will act in accordance with the provisions of the deposit agreement to ensure that the data can still be accessed.